White paper

Detecção contínua de ameaças contra o endpoint e resposta em um momento específico.

Resumo

A única maneira de acabar com as ameaças de segurança de hoje é tratá-la como um todo durante o ciclo do ataque; antes, durante e depois do ataque. É fundamental para este modelo que a Cisco aplique a abordagem de análise contínua do endpoint em conjunto com uma arquitetura de Big Data . As inovações em relação à proteção avançada contra malware incluem:

- Análise contínua
- Retrospecção
- Indicações comportamentais de comprometimento
- Trajetória do dispositivo e arquivo
- Controle de ataques
- Baixa predominância

Quando esses recursos são combinados a um fluxo de trabalho integrado, o impacto real na detecção, no monitoramento, na análise, na investigação e na contenção do malware torna-se evidente.

Um novo modelo de proteção para o endpoint

A Cisco não é nova na área de inovação de segurança e nem fica parada enquanto os invasores se modernizam. Na verdade, já em 2003, nós (como a antiga Sourcefire) tínhamos uma visão sobre o que seria necessário para combater as ameaças avançadas e fomos pioneiros no conceito de descoberta de rede contínua, que se tornou o alicerce dos sistemas de prevenção de intrusão de próxima geração (NGIPSs). Hoje, o malware avançado direcionado e os ataques sofisticados são constantes e comprometem os ambientes ao utilizar técnicas novas e furtivas. Mais uma vez, a Cisco está mudando a forma de lidar com a segurança. Estamos desenvolvendo recursos contínuos e introduzindo um novo modelo para combater os ataques.

Proteção contínua em um mundo dinâmico

Quando a Sourcefire (agora parte da Cisco) iniciou, há mais de uma década, a visibilidade da rede em tempo real, o padrão para a visibilidade de rede era usar ferramentas de verificação invasivas em momentos específicos. Essas ferramentas levavam um tempo considerável para realizar uma análise completa e eram prejudiciais para a rede e os sistemas verificados. A natureza dinâmica das redes tornava a coleta de dados mais problemática, pois eles tornavam-se desatualizados com rapidez e, por isso, o processo inteiro precisava ser realizado repetidas vezes. Por fim, os dados eram repletos de pontos cegos e difíceis de correlacionar com os dados das ameaças ativas.

A Cisco reconheceu que o principal problema de segurança que muitos defensores enfrentam não é o de proteger o seu ambiente, mas de compreender suficientemente o que estão protegendo e como estão organizados, para que possam dar início ao processo contínuo de proteção, conforme sua evolução. Com o contínuo conhecimento da rede em tempo real, a visibilidade pode, pela primeira vez, ser totalmente integrada à detecção de ameaças, o que mudará a defesa contra as ameaças à rede para sempre. O conhecimento da rede em tempo real tornou-se um requisito fundamental para NGIPS, conforme definido pelo Gartner, e faz parte da tecnologia FireSIGHT™ da Cisco.

Em 2013, também foi apresentado mais um modelo de segurança com mudança de paradigma, para enfrentar a infestação de ameaças avançadas. Com base no conceito de que o cenário de ameaças e o ambiente de TI de hoje são dinâmicos e estão em constante expansão, este novo modelo de segurança lida com todo o ciclo de ataque; antes, durante e depois do ataque.

Com base no conhecimento da rede em tempo real, a metodologia tradicional de um momento específico está se transformando em uma abordagem contínua. Esse modelo:

- Promove uma inovação única na batalha contra as ameaças avançadas de hoje
- Proporciona visibilidade em relação ao comprometimento e à persistência do ataque como nunca antes
- Permite que as equipes de segurança contenham e corrijam com rapidez e precisão a infecção sem atrapalhar os usuários finais e a equipe de segurança
- Capacita as equipes de segurança para serem caçadoras e não a caça

Expectativa de resultados diferentes

O mundo da detecção e resposta às ameaças de endpoint está repleto de marcas e mensagens de alto nível que parecem iguais. Todos dizem liderar a próxima revolução na detecção de malware. Muito semelhante aos scanners de rede antigos, cada empresa afirma oferecer mais proteção contínua e em tempo real do que as outras, quando na realidade são apenas melhorias incrementais na mesma ferramenta com as mesmas limitações fundamentais.

> Insanidade: fazer a mesma coisa diversas vezes e esperar resultados diferentes.
>
> – Albert Einstein

As melhorias mais recentes na detecção de ameaças envolveram a execução de arquivos em um sandbox para detecção e análise, o uso de camadas virtuais de emulação para ofuscar o malware de usuários e sistemas operacionais e o uso da lista de permissão da aplicação com base na reputação para diferenciar as aplicações aceitáveis das mal intencionadas. Mais recentemente, entraram em cena a simulação da cadeia de ataque e a detecção de análise. Mas os invasores conhecem a natureza estática dessas tecnologias de segurança e, como era de se esperar, estão inovando em torno das limitações delas para penetrar nas defesas da rede e do endpoint.

Infelizmente, foi o usuário que obteve menos melhorias revolucionárias em relação à tecnologia de detecção de ponta do ano passado, e o ciclo se repete sem abordar a limitação subjacente. A tecnologia de detecção de hoje está parada no tempo: em um momento específico para ser exato.

O malware é dinâmico e tridimensional. Ele não existe em um terreno bidimensional ‘X-Y’ de um momento específico, que aguarda para ser detectado, onde X representa o tempo e Y o mecanismo de detecção. O malware existe como um ecossistema interconectado que está em movimento constante. Até mesmo para ser remotamente eficaz, as defesas têm de ser multidimensionais e tão dinâmicas quanto o malware, levando em consideração, também, as relações entre os diferentes tipos de malware. Temos que deixar de lado a esperança de que uma tecnologia de detecção hiper avançada extinguirá o problema.

O que é necessário é uma mudança verdadeiramente transformadora na maneira como abordamos a detecção de ameaças avançadas e atividades de violação. Precisamos de proteção e visibilidade contínuas, desde o ponto de entrada, até a propagação e a reparação após a infecção.

Um modelo contínuo e autêntico responde às questões mais importantes

- Qual foi o método e o ponto de entrada?
- Quais sistemas foram afetados?
- O que a ameaça fez?
- Posso interromper a ameaça e sua causa inicial?
- Como me recuperar da ameaça?
- Como evitar que isso ocorra novamente?
- Posso detectar com rapidez as IoCs antes de afetarem a minha empresa?

Mudança de paradigma em um momento específico

O malware avançado de hoje compromete os ambientes com uma ampla variedade de vetores de ataque, assume infinitos formatos, lança ataques ao longo do tempo e pode confundir o vazamento de dados. Com o desenrolar da invasão, ele deixa um enorme rastro de dados que podemos captar, armazenar, manipular, analisar e gerenciar, a fim de compreender esses ataques e saber como derrotá-los. Com base em um modelo de disponibilização da proteção antes, durante e depois de um ataque, a solução de proteção avançada contra malware (AMP) da Cisco® para endpoints combina uma abordagem contínua com uma arquitetura de Big Data para superar as limitações das tecnologias tradicionais de detecção e resposta em um momento específico.

Nesse modelo, os dados de telemetria do processo são coletados continuamente enquanto ocorrem em todas as fontes e são sempre atualizados, conforme necessário. A análise pode ser feita em camadas para trabalhar em conjunto e eliminar os impactos sobre os pontos de controle e para disponibilizar níveis avançados de detecção durante um período prolongado. A análise envolve mais do que a enumeração e correlação de eventos; também significa entrelaçar os dados de telemetria para obter uma perspectiva maior sobre o que está acontecendo em todo o ambiente. Ao atingir uma comunidade mais ampla de usuários, a Inteligência coletiva de segurança da Cisco é continuamente atualizada a nível mundial e compartilhada imediatamente. Essa inteligência global está correlacionada aos dados locais, para uma tomada de decisão ainda mais informada.

Neste modelo, a detecção e resposta não são mais disciplinas ou processos distintos, mas uma extensão do mesmo objetivo: interromper as ameaças avançadas antes que elas detenham você. Os recursos de detecção e resposta são contínuos e integrados e vão além de metodologias tradicionais em momentos específicos.

Benefícios da análise contínua

- Menos foco na detecção de dados
- Automação da análise avançada
- Melhor priorização da ameaça
- Tempo mais rápido para reparação

Detecção

Nenhum método de detecção é 100% eficaz, pois os invasores continuam a inovar para fugir dessas defesas de linha de frente. No entanto, apesar das limitações da detecção em um momento específico, ela mantém um papel importante na eliminação de uma grande maioria de ameaças em potencial. Além disso, através da aplicação de uma abordagem contínua à detecção tradicional, os defensores podem melhorar as tecnologias em um momento específico, tornando-as mais eficazes, eficientes e difundidas.

Mas isso é apenas o começo de como a abordagem contínua da Cisco transforma a proteção avançada contra malware. Mais importante, ela nos permite disponibilizar uma variedade de outras inovações que melhoram todo o processo de proteção avançada contra malware, da detecção à resposta.

Recursos contínuos viabilizam a inovação

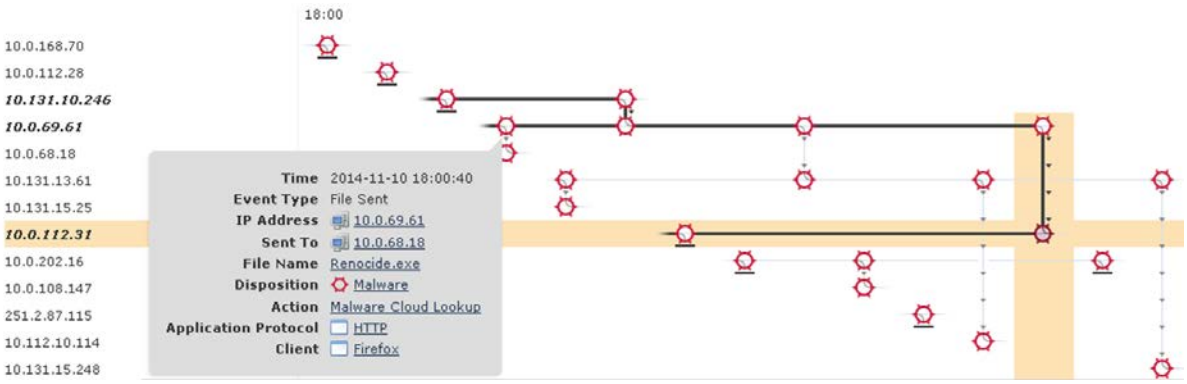
A única maneira de defender-se contra as ameaças avançadas de hoje é tratá-las globalmente durante todo o ciclo do ataque; antes, durante e depois do ataque. Nossa abordagem contínua, em conjunto com uma arquitetura de Big Data é fundamental para esse modelo e permite uma variedade de inovações adicionais na proteção avançada contra malware, incluindo:

- **Retrospecção**: a possibilidade de conduzir a análise em um momento específico no início e ao longo de um período prolongado não é limitada aos arquivos. Também inclui processos, comunicações e outros dados de telemetria, algo que os modelos tradicionais em um momento específico simplesmente não podem enfrentar.
- **Entrelaçamento da cadeia de ataque**: o método para entrelaçar os fluxos de retrospecção do arquivo, processo e comunicação à medida que acontecem, para capturar a dimensão relacional, está ausente nas tecnologias bidimensionais em um momento específico.
- **Indicações comportamentais do comprometimento (IoCs)**: são mais que artefatos estáticos. São indícios comportamentais complexos que o entrelaçamento da cadeia de ataque captura em tempo real, e os IoCs comportamentais os detectam à medida que ocorrem em tempo real.
- **Trajetória**: é mais do que um termo de marketing sofisticado para o monitoramento. O monitoramento produz uma lista enumerada de eventos em momentos específicos para mostrar a trajetória. A “trajetória” refere-se ao caminho adjacente em que um objeto, neste caso o malware, move ao longo do tempo. É substancialmente mais eficaz em mostrar o escopo e as causas iniciais do malware, em relação ao caminho percorrido e as suas consequências.
- **Busca de ameaças:** com a análise oportuna da natureza dinâmica do malware e a amplitude dos dados sempre atualizada, a capacidade de direcionar todas as atenções pra os IoCs de malware evasivo é tão simples quanto procurar seu restaurante favorito no Google.

É importante pois cada uma dessas inovações serve especificamente para combater o malware e as ameaças avançadas que ele representa. E quando combinadas a um fluxo de trabalho integrado, o impacto real torna-se evidente através da detecção, do monitoramento, da análise, da investigação e da contenção do malware.

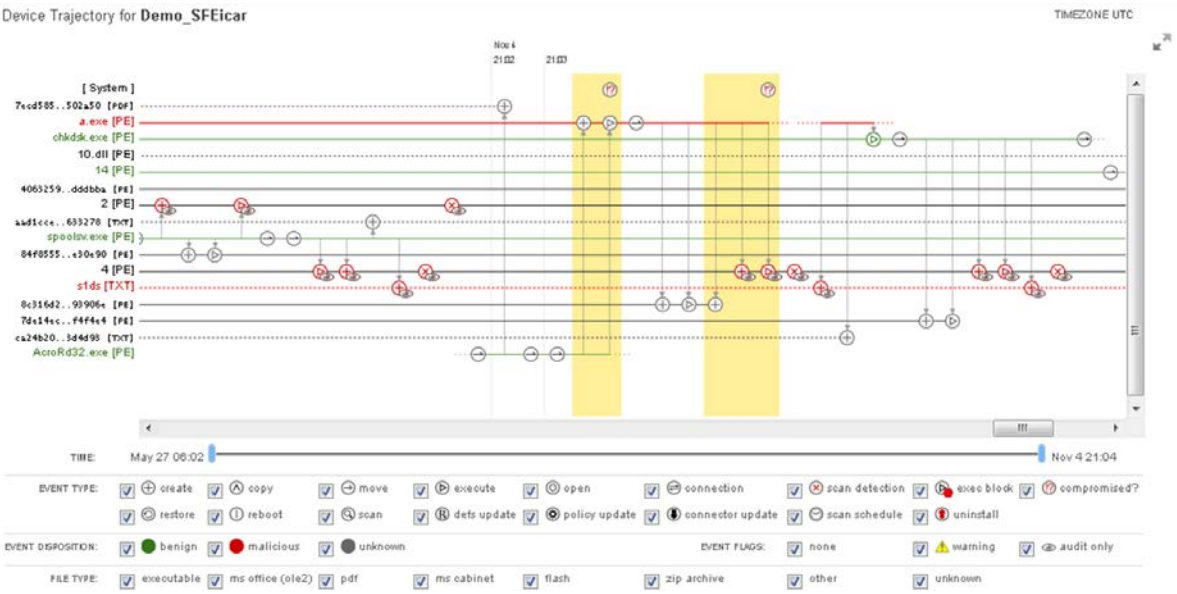
A Figura 1 mostra a propagação de malware com informações sobre o ponto de entrada, atividade do malware e os endpoints afetados.

Figura 1. Tela de trajetória do arquivo de rede da AMP da Cisco



A Figura 2 mostra uma propagação de malware na tela de trajetória do dispositivo com informações sobre o ponto de entrada, atividade do malware e os binários e executáveis que afetam um endpoint específico. Esta informação é correlacionada e compartilhada entre os endpoints em toda a rede estendida e integrada com a exibição da rede na Figura 1.

Figura 2. Tela de trajetória do dispositivo da AMP para endpoints da Cisco



Monitoramento

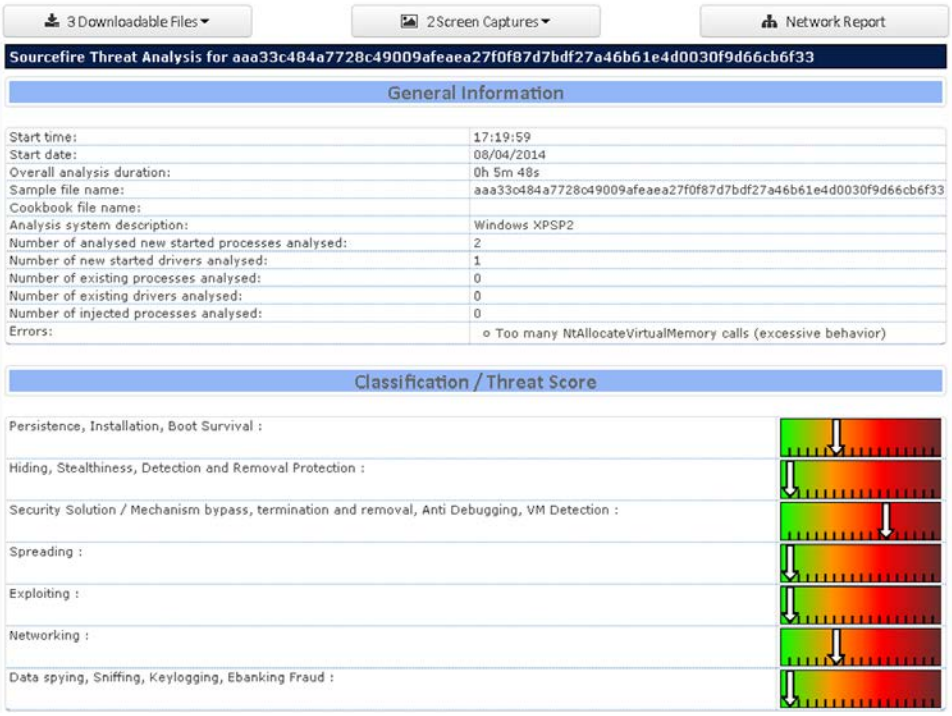
A retrospecção é um recurso com a capacidade de coletar os dados de telemetria do endpoint e analisá-los em busca de atividades de ameaça enquanto ocorre e durante um período prolongado. A Cisco foi a primeira a apresentar essa inovação. É um grande avanço da coleta de dados orientada por eventos ou verificações agendadas para novos dados, e captura os ataques conforme ocorrem, da mesma maneira que um sistema de vigilância por vídeo.

Análise avançada automatizada

Para detectar ataques avançados enquanto se movem lateralmente através da rede e pelos endpoints, os defensores precisam de tecnologias que procuram automaticamente os IoCs esquecidos por malware e exploradores, assim como os comportamentos de comprometimento mais avançados que acontecem ao longo do tempo. A abordagem contínua da Cisco disponibiliza esse nível de automação por meio de recursos avançados de detecção de comportamento, não com o objetivo de fornecer mais uma lista de alertas para investigar, mas sim, para disponibilizar uma visão priorizada e agrupada das melhores áreas de comprometimento e atividade de violação. Com a análise de Big Data e o uso de recursos e padrões contínuos, os IoCs podem ser identificados à medida que surgem, para que as equipes de segurança possam concentrar seus esforços nas ameaças que apresentam o maior potencial de dano.

A Figura 3 mostra informações detalhadas sobre o comportamento do arquivo, inclusive a gravidade dos comportamentos, o nome do arquivo original, as capturas de tela do malware em execução e exemplos de capturas de pacotes. Com essas informações, você terá uma compreensão melhor do que é necessário para conter os ataques e bloqueá-los futuramente.

Figura 3. Tela de análise do arquivo da AMP para endpoints da Cisco



Busca de ameaças em comparação com Investigação

Sem o contexto e os recursos de uma abordagem contínua, o termo “investigação” pode provocar movimentos involuntários das equipes de segurança com experiência no processo trabalhoso de tentar localizar uma não conformidade com pouca evidência contextual. Muitas vezes, a pergunta mais difícil de ser respondida é: “Por onde vamos começar?”. Em uma abordagem contínua, as investigações podem ser mais rápidas, direcionadas e produtivas.

Uma abordagem contínua deixa de ser uma pesquisa por fatos e pistas evasivas para ser uma busca muito focada em violações baseadas em eventos reais, como detecções de malware e IoCs estáticos e comportamentais. Recursos contínuos apoiados por uma arquitetura de big data permitem que todos os dados sejam pesquisados facilmente a qualquer momento. Em um modelo contínuo que utiliza os recursos previamente discutidos (inclusive as detecções comportamentais e para momentos específicos, assim como a retrospecção), a busca por malware pode ser rápida e eficaz. A investigação ou a busca por ameaças envolve a compreensão visual do ponto de entrada, extensão e causas iniciais da infecção. Também inclui o recurso para identificar um cronograma para a busca, expandir ou reduzi-lo e identificar e alternar a busca com filtros. Este recurso torna-se uma ferramenta importante e um multiplicador eficiente, à medida que as equipes de segurança se movem da resposta às cegas aos alertas e incidentes para a busca rápida por malwares antes que um ataque se intensifique.

O controle de ataques em comparação com custos

A investigação pode parecer complicada, se for limitada pela detecção para momentos específicos e tecnologias forenses. Assim como a noção de conter o malware ou a suspeita de malware, sem a necessidade da reinstalação. Como as tecnologias para momentos específicos não enxergam a cadeia de eventos e as informações contextuais que as acompanham, a capacidade de conter o malware de forma precisa não está nem mesmo dentro das possibilidades.

Com a visibilidade que a abordagem contínua proporciona, combinada com a capacidade de direcionar as causas iniciais específicas, romper a cadeia de ataque não é apenas rápido, mas fácil. Além do mais, mesmo que o procedimento operacional padrão seja a reinstalação de um dispositivo gravemente comprometido, toda a detecção e os dados de telemetria ainda estarão preservados e a contenção ainda poderá ser executada para evitar um comprometimento futuro por invasores que usam o mesmo gateway da infecção.

Por fim, as tecnologias tradicionais para momentos específicos, às vezes, falham ao detectar um ataque, e uma empresa pode se encontrar em meio a uma violação ativa. Especificamente, muitos endpoints foram infectados por um longo período e a equipe de resposta a incidentes tem se engajado em investigar e corrigir a situação. Tal como a detecção e descoberta, o tempo é essencial neste cenário, e as mesmas perguntas de base aplicam-se: “Por onde começamos?" e "A situação é muito ruim?”. No entanto, responder e conter o ataque neste cenário, muitas vezes, envolve compreender com rapidez a extensão e as causas iniciais, sem mostrar-se vulnerável aos invasores. Para prevenir os movimentos laterais de um invasor é essencial fechar rapidamente todos os pontos de comprometimento e os gateways de infecção simultaneamente.

Desde o momento da implantação, uma abordagem contínua inicia imediatamente a coleta das informações vitais de detecção e telemetria, que ajudarão a equipe de resposta a compreender a gravidade do ataque, onde estão os hotspots e, o mais importante, estabelecer um perfil de contenção que pode ser invertido instantaneamente. A detecção comportamental avançada, o rastreamento e a visualização iniciam imediatamente e estão em modo de auditoria, ao contrário dos processos em um cenário de detecção e proteção. Eles ainda detectam e alertam, mas em vez de bloquear ativamente o malware, capturam a evidência como detetives em uma emboscada que reúnem informações para a equipe da SWAT aproveitar e encerrar a operação.

A diferença fundamental entre uma resposta contínua e em um momento específico é que a primeira fornece um recurso de controle de ataques sólido, que inclui uma contenção precisa, enquanto uma resposta em um momento específico só disponibiliza listas de fatos e evidências enumeradas. Embora essas listas possam ser usadas por equipes de segurança, é trabalhoso torná-las úteis para a contenção.

Integração e relatórios

A Cisco AMP para endpoints foi projetada desde o início para apoiar uma abordagem contínua e uma arquitetura de Big Data. Ela usa um modelo em nuvem para viabilizar um conector leve, em vez de uma arquitetura de agentes pesada no endpoint. O conector é semelhante a um coletor de dados de arquivo e telemetria, em vez de um agente de detecção pesado, com extensão e eficácia limitados por impactos da computação e memória sobre os endpoints e usuários. Este modelo libera recursos para que o conector possa monitorar continuamente, coletar e transmitir de forma eficiente os dados de telemetria para a nuvem para análise de Big Data.

O modelo de conector leve também viabiliza os conectores para serem compatíveis com uma variedade de plataformas de endpoint, como Windows, Mac, Android e ambientes virtuais, com um alto nível de paridade entre plataformas. Esta conectividade estende a detecção e proteção de malware em outros pontos de controle, como e-mail e dispositivos de gateway da Web, sistemas de prevenção contra invasões, firewalls e serviços em nuvem de próxima geração, com altos volumes de transações de arquivo.

A coleção abrangente e a análise avançada de dados do arquivo e telemetria nos pontos de controle de acesso enriquecem o nível de inteligência coletiva que pode ser compartilhada localmente dentro de um ambiente e globalmente com clientes através da mais ampla Nuvem de inteligência coletiva da Cisco. O compartilhamento de informações em tempo real ajuda as equipes de segurança a se manterem à frente de ataques amplos que utilizam técnicas como phishing, em que muitos usuários podem ser infectados com a mesma carga inicial, mas, em seguida, recebem diferentes downloads ou comandos subsequentes. Além da análise de dados do arquivo, outros dados de telemetria podem ser analisados através de pontos de controle para determinar com mais precisão a extensão do ataque.

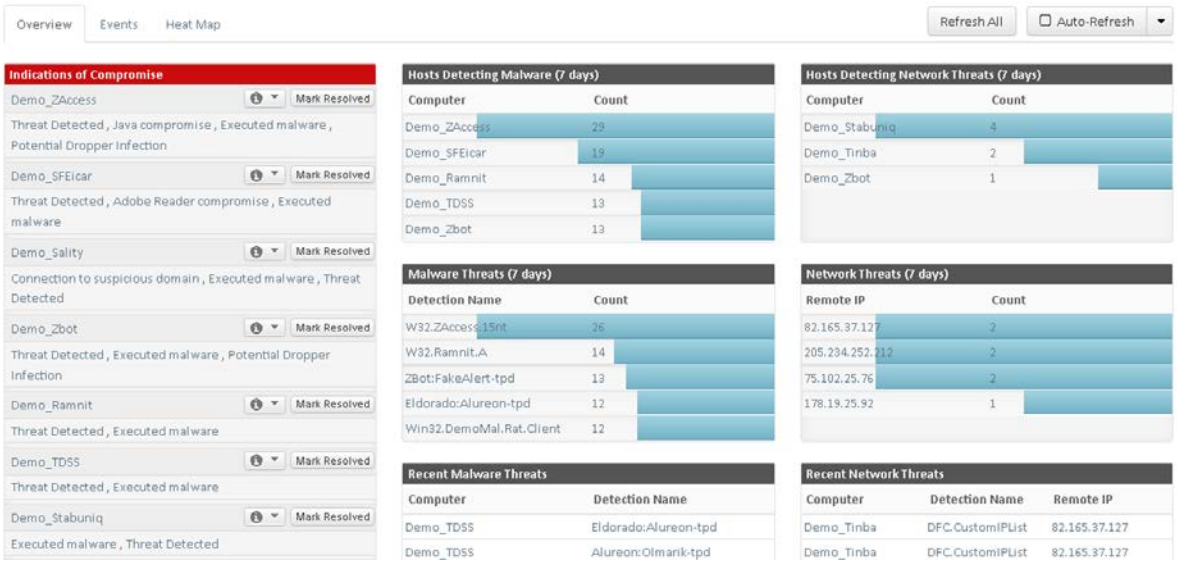
Uma vez na nuvem, os detalhes das informações de telemetria coletadas através de pontos de controle de acesso podem ser compartilhados com todos os pontos de controle para fornecer informações contextuais da mesma forma, mesmo em pontos de controle que não consigam coletar esse nível de informação. Por exemplo, os dados de telemetria e as detecções de comportamento coletados de um endpoint podem ser usados por equipes de segurança de rede para determinar a extensão da exposição a um malware específico. Do endpoint, as informações que indicam se o arquivo foi baixado, aberto ou até mesmo movido podem fornecer um quadro mais completo para as equipes de segurança, do que os dados de alerta genéricos. Os endpoints que ativaram o malware terão uma prioridade mais alta do que aqueles que só fizeram o download. As importantes informações contextuais do endpoint compartilhadas em tempo real com outros pontos de controle para uma melhor determinação da ameaça e suporte à decisão estão em nítido contraste com a lista típica e simples de eventos que podem ou não ser ameaças reais.

Uma abordagem contínua também se estende aos recursos de geração de relatório. Os relatórios não são mais limitados à enumeração e agregação de eventos. Eles podem incluir painéis e tendências acionáveis que destacam a relevância dos negócios e os possíveis riscos. Embora as tecnologias para momentos específicos também possam fornecer painéis e relevância do risco, elas normalmente exigem uma camada adicional de complexidade na forma de inteligência da segurança e gerenciamento de eventos (SIEM) para filtrar e correlacionar o grande volume de dados do evento.

Uma arquitetura de Big Data lida com o volume cada vez maior de dados que são essenciais para a detecção e análise eficaz de malware, enquanto uma abordagem contínua usa esses dados para fornecer o contexto e, mais importante, priorizar quando e onde serão utilizados.

A Figura 4 mostra os painéis e as tendências acionáveis da Cisco AMP para endpoints que destacam a relevância dos negócios e o impacto de uma perspectiva de risco. Os relatórios não são limitados à enumeração e agregação de eventos. Nesta exibição, vemos indicações priorizadas de comprometimento, hosts que detectam o malware e ameaças de rede, entre outros dados.

Figura 4. Painéis da Cisco AMP para endpoints



Conclusão: é verdade, 1 + 1 não é igual a 3. Às vezes, somam 6.

Uma abordagem contínua em conjunto com uma arquitetura de Big Data possibilita seis grandes áreas de inovação revolucionária na batalha contra as ameaças avançadas que visam o endpoint:

1. **A detecção vai além de momentos específicos.** Uma abordagem contínua permite que a detecção se torne mais eficaz, eficiente e abrangente. Os métodos de detecção de comportamento, como sandboxing, são otimizados, a atividade é supervisionada enquanto ocorre e a inteligência é compartilhada entre os mecanismos de detecção e pontos de controle.
2. **Monitoramento que viabiliza o entrelaçamento de cadeia de ataques.** A retrospecção, o monitorando contínuo de arquivos, processos e comunicações e, em seguida, o entrelaçamento dessas informações para criar uma linhagem de atividades, fornece informações sem precedentes sobre um ataque, à medida que ele ocorre.
3. **Análise avançada automatizada que monitora os comportamentos ao longo do tempo.** A combinação da análise de Big Data e dos recursos contínuos para identificar padrões e IoCs à medida que surgem, ajuda as equipes de segurança a focar nas ameaças mais perigosas.
4. **A investigação que transforma a caça em caçador.** Transformar as investigações em buscas centradas em ameaças baseadas em eventos e IoCs reais fornece às equipes de segurança uma forma rápida e eficaz para compreender e verificar a extensão de um ataque.
5. **A contenção é realmente simples.** Romper a cadeia de ataque é rápido e eficaz com o nível de visibilidade que a abordagem contínua oferece, combinada à capacidade de direcionar as causas específicas.
6. **Painéis acionáveis e contextuais.** Relatórios que são baseados na coleta abrangente e análise avançada de dados do arquivo e telemetria através dos pontos de controle e, em seguida, são sobrepostos com informações contextuais, destacam tendências, relevância dos negócios e impactos sobre o risco.

A Cisco está disponibilizando um novo modelo para lidar com os ataques avançados de hoje, com base nos esforços pioneiros em recursos contínuos e na combinação com uma arquitetura de Big Data. Neste modelo, a detecção e resposta não são mais disciplinas ou processos distintos, mas uma extensão do mesmo objetivo: interromper as ameaças avançadas antes que elas detenham você. Os recursos de detecção e resposta são contínuos e integrados e vão além de metodologias tradicionais em momentos específicos. É o necessário para a detecção e resposta de ameaças de endpoint para o mundo real.

Comparação entre a abordagem contínua e o modelo para um momento específico

A seguir, encontram-se comparações detalhadas de recursos que diferenciam uma abordagem contínua de um modelo para um momento específico. As descrições também abordam melhorias na detecção, bem como inovações em relação à proteção avançada contra malware.

Tabela 1. Detecção

Abordagem contínua	Modelo para um momento específico
• Uma estrutura integrada de mecanismos pode trabalhar em conjunto, ao compartilhar o contexto para obter recursos de detecção aperfeiçoados. • Os métodos de detecção comportamentais, como sandboxing, são otimizados ao reduzir as cargas de trabalho e latência e eliminar a necessidade de uma área restrita a cada novo arquivo. • A detecção é realizada durante um período prolongado, que é exatamente como os ataques ocorrem ao longo do tempo. • O modo de auditoria é transformado de um parâmetro de ajuste simples usado para reduzir os falsos positivos em uma ferramenta de coleta de resposta a incidentes para capturar as atividades em tempo real, sem avisar os invasores. • A inteligência de detecção é compartilhada coletivamente e de forma instantânea através de pontos de controle múltiplos.	• Os mecanismos, se houver mais de um, funcionam como uma pilha, ao operarem em série e de forma independente, o que reduz a eficácia e diminui o desempenho no endpoint. • São necessárias atualizações do fornecedor, o que requer tempo e cria mais lacunas na segurança.

Tabela 2. Monitoramento

Abordagem contínua	Modelo para um momento específico
• Retrospecção do arquivo: após a análise de detecção inicial, um arquivo continua a ser investigado por um longo período com os recursos de detecção e inteligência de ameaças coletivas mais recentes. Uma disposição atualizada pode, assim, ser processada e uma análise mais completa pode ser conduzida além do momento em que o arquivo foi visto pela primeira vez. • Retrospecção do processo: semelhante à retrospecção do arquivo, a retrospecção do processo é a capacidade de captar e analisar continuamente o I/O do processo do sistema, por um longo período, para a análise da cadeia de ataque e detecção comportamental do IoC. • Retrospecção de comunicação: as comunicações de e para um endpoint são captadas continuamente, assim como a aplicação e o processo associados que iniciaram ou receberam a comunicação. Essas informações fornecem dados contextuais adicionais como parte da análise da cadeia de ataque e detecção comportamental do IoC. • Entrelaçamento do ataque em cadeia: o Cisco AMP para endpoints faz mais do que a retrospecção; ele apresenta um novo nível de inteligência através do entrelaçamento de várias formas de retrospecção em uma linhagem de atividades que está disponível para análise em tempo real, a qualquer momento em que for necessária. Especificamente, as diferentes formas de retrospecção podem ser entrelaçadas através da análise para procurar padrões de comportamento de um endpoint específico ou em toda a comunidade de endpoints.	• Sem retrospecção: o modelo é indiferente à atividade relacional no endpoint, além da atividade de detecção. • O modelo também é completamente indiferente a tudo o que acontece dentro da rede, depois que o malware passa pelo ponto de controle.

Tabela 3. Análise avançada automatizada

Abordagem contínua	Modelo para um momento específico
• Resposta em tempo real: como os dados de telemetria do endpoint são continuamente coletados e adicionados ao armazenamento, eles podem ser comparados automaticamente com os IoCs estáticos e comportamentais. O tempo de detecção de um IoC estático ou comportamental pode, portanto, ser drasticamente reduzido. • Indicações comportamentais do comprometimento (IoCs): ao usar o entrelaçamento do ataque em cadeia, os IoCs comportamentais procuram padrões sofisticados de atividade em todos eventos de detecção, IoCs estáticos e dados de telemetria que indicam um possível comprometimento. Um exemplo clássico é um conta-gotas que passou pela detecção inicial. • Entrelaçamento do ataque em cadeia: também registra o que aconteceu antes e depois do acionamento do IoC comportamental. A equipe de segurança pode alternar com rapidez de um alerta significativo a uma plena compreensão da extensão de um ataque e a capacidade de conter o problema com precisão. • IoCs abertos: com os IoCs abertos, os clientes podem usar suas listas de detecção de IoC estático personalizadas. • IoCs baseados em inteligência: mais do que uma inteligência estática, listas de bloqueio ou scripts de detecção, esses IoCs são baseados em algoritmos comportamentais que buscam ações mal intencionadas específicas e relacionadas ao longo do tempo. Os IoCs baseados em inteligência são desenvolvidos e totalmente respaldados pelo Cisco Talos Security Intelligence e o Research Group. • Predominância: um mecanismo de análise avançada determina a predominância de um malware detectado em relação à empresa e à comunidade global mais ampla. Muitas vezes, os arquivos mal-intencionados com baixa predominância são indicativos de malwares direcionados e uma tentativa específica de comprometimento. Isso normalmente é ignorado pelas equipes de segurança. A análise de predominância destaca esses tipos de ataques, especialmente se correlacionados com outros IoCs estáticos ou comportamentais que envolvem esses sistemas.	• Algumas tecnologias para momentos específicos podem procurar por artefatos de IoC estáticos, mas não podem fazer isso em tempo real e muitas vezes exigem uma coleta de dados demorada antes que o IoC possa ser executado. • Este modelo pode mostrar quantas vezes ou onde o malware foi visto, mas carece de informações relacionadas às causas iniciais. • O significado ou a predominância da ameaça não são exibidos. • Se não existirem recursos de predominância, eles não podem ser implementados em tempo real, nem podem continuar a monitorar um arquivo, processo ou mesmo uma comunicação específica. • Os IoCs comportamentais não podem ser identificados.

Tabela 4. Busca de ameaças em comparação com Investigação

Abordagem contínua	Modelo para um momento específico
• Trajetória do arquivo: a extensão da exposição a arquivos mal-intencionados ou suspeitos é rapidamente entendida com o tempo, método e ponto de entrada; os sistemas afetados e a predominância, tudo sem a necessidade de verificar ou fazer capturas instantâneas de endpoints. • Trajetória do dispositivo: com base no nível de extensão fornecido pela trajetória do arquivo, a trajetória do dispositivo disponibiliza uma sólida análise da janela de intervalo nos processos do sistema para entender o histórico da causa inicial e a linhagem. Ela também pode expandir ou reduzir o cronograma e filtrá-lo para identificar com rapidez a causa exata do comprometimento. • Pesquisa flexível: fornece um método rápido e simples de perguntar; “Onde mais esse indicador foi visto?”, sem os limites típicos de consultas de banco de dados relacional. Tudo, do nome do host, nome do arquivo, URL e endereço IP até strings de texto, pode ser pesquisado em todo o conjunto de dados e através da inteligência coletiva global. Considerando os milhões de arquivos que são analisados constantemente, ela se torna uma ferramenta eficaz para buscar com rapidez ameaças avançadas, antes que seja tarde demais. • Análise do arquivo: primeiramente, o modelo oferece um mecanismo seguro para executar um arquivo em um sandbox, a fim de analisar completamente o comportamento e classificar o nível de ameaça do comportamento. Em segundo lugar, ele fornece o resultado da análise em um relatório detalhado. Terceiro, todos os resultados da análise são adicionados à inteligência coletiva. E quarto, todos os resultados da análise podem ser pesquisados na pesquisa flexível. Mais uma vez, as equipes de segurança podem alternar com rapidez de um indicador, em um relatório de análise do arquivo, à verificação de onde encontrá-lo na empresa. Isso é extremamente importante quando um ataque é direcionado mas utiliza um método de infecção genérico.	• É nessa hora que as tecnologias tradicionais de detecção para momentos específicos se mostram ineficazes. Elas não fornecem nenhum monitoramento pós detecção ou informação contextual. ◦ As detecções são frequentemente captadas em eventos independentes que são adicionados a uma lista enumerada por evento. Sim, a lista é atualizada constantemente, mas sem qualquer retrospecção contextual. ◦ Não há recursos de visualização dos eventos antes e depois da detecção. ◦ Não há recursos para analisar completamente os arquivos por comportamento e, em seguida, procurar rapidamente em todos os endpoints por IoCs específicos. • Algumas tecnologias podem fornecer recursos limitados (por exemplo, para determinar quando e onde o malware foi detectado com base nos dados de enumeração do evento), mas não têm a capacidade de colocar eventos na janela de intervalo para períodos antes e após o comprometimento. • As ferramentas tradicionais forenses e de investigação para momentos específicos não são melhores do que as suas equivalentes, mesmo que afirmem ser contínuas. ◦ Elas carecem de quaisquer meios avançados de detecção de ameaças. A detecção, se combinada à informação contextual contínua, pode ser um importante ponto de partida, mas as ferramentas forenses são criadas para encontrar artefatos e pistas, não relações. ◦ Elas não têm a capacidade de fornecer a visualização das janelas de intervalo de eventos, antes e depois de um comprometimento. ◦ Também não têm a capacidade de pesquisar rapidamente por IoCs específicos, sem a necessidade de atualizar todos os dados.

Tabela 5. O controle de ataques em comparação com custos

Abordagem contínua	Modelo para um momento específico
• Contenção simples: você suspeita que um arquivo seja mal-intencionado? Nenhum problema e nenhuma espera. Use a codificação SHA256 do arquivo (algoritmo hash seguro) para bloqueá-lo imediatamente com poucos cliques em todos os endpoints, em um grupo de endpoints ou apenas em um endpoint. • Contenção avançada: similar aos scripts Snort®, as detecções avançadas personalizadas dão a possibilidade de lidar com as famílias de malware, sem a espera de uma atualização de assinatura. • Listas negras e brancas de aplicações: com informações contextuais valiosas, as listas de controle podem ser usadas para determinar de forma mais eficaz se aplicações bem intencionadas estão sendo usadas como gateways para atividades maliciosas, e interromper aplicações mal-intencionadas. Estas listas se prolongam à análise contínua e aos dados de telemetria. As equipes de segurança podem controlar com rapidez a situação, enquanto os procedimentos padrão para a resposta são aplicados. • Lista de bloqueio de IP: semelhante às listas de controle de aplicações, as listas de bloqueio de IP podem ser utilizadas de forma mais eficaz no caso de um evento real ou em políticas corporativas para controlar um ataque e monitorar os endpoints para as comunicações suspeitas provenientes de um endpoint. Este recurso é extremamente importante no cenário da violação, onde qualquer comunicação cruzada utilizada por um invasor precisa ser extinguida quando o plano de contenção for implementado.	• As tecnologias para momentos específicos são bastante limitadas em sua capacidade de conter o malware ou os suspeitos de malware, porque são projetadas para se concentrar no ponto de detecção e não mais tarde durante o ciclo do ataque, onde a contenção é um requisito fundamental. • Algumas tecnologias de detecção para momentos específicos capacitam a lista de bloqueio de aplicações. Este é um bom método para conter aplicações que representam um risco para uma empresa ou aplicações suspeitas que ainda não foram determinadas como bem ou mal-intencionadas, mas devem ser bloqueadas como precaução. No entanto, a lista de bloqueio é mais eficaz quando é informada por um conjunto robusto de recursos de detecção comportamental e de arquivo para executar as funções primárias de detecção, análise e contenção. As maiores desvantagens são que o gerenciamento destas tecnologias como uma camada primária de proteção torna-se incrivelmente trabalhoso, elas são propensas a deixar passar os ataques e são indiferentes às atividades de ataques em cadeia. • Por fim, as ferramentas forenses e de resposta para momentos específicos não são criadas para o controle rápido de ataques , necessário para os tipos de ameaças avançadas encontradas hoje. Elas são úteis em uma investigação, mas não conseguem alternar entre a enumeração de dados e a contenção. Muitas vezes, essa etapa exige uma atividade trabalhosa, que normalmente é evitada pela abordagem de reinstalação mais simples.

Para mais informações

Para saber mais sobre a abordagem de segurança da Cisco, envie um e-mail para ciscosecurityinfo@cisco.com ou ligue para 800 553-6387.

Sede - Américas
Cisco Systems, Inc.
San Jose, CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pte, Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam.
Holanda

A Cisco tem mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site **www.cisco.com/go/offices**.

Impresso nos EUA C11-733649-00 02/15